Cyber Analysis and Visualization Environment (CAVE)

Jeremy Pecharich, Ph.D.
Cybersecurity Engineer
Cyber Defense
Engineering and Research, Group

Jet Propulsion Laboratory
California Institute of Technology

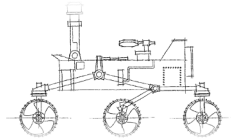
Goal/ Primary Question

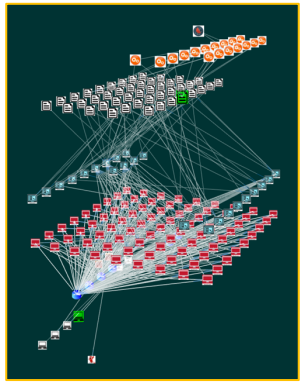
How do we use model-based engineering concepts to effectively perform a cyber-risk assessment that takes into account mission objectives?

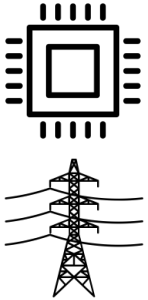
Cyber Defense Engineering and Research

Tasks and responsibilities, past and present

- Project/Program Office Cyber Defense Engineering
- Supports Cyber Security Improvement Project
- Non-NASA Reimbursable tasks (Power Grid, Oil and Gas, DoD)







- Fundamental research in Cyber Security
- Technology development
  - System Modeling and Analysis
  - Cyber/cyber-physical experiment test execution and validation
  - Hardware and software security technology transition to Industry
  - JPL Flight avionics with built-in security architectural provisions

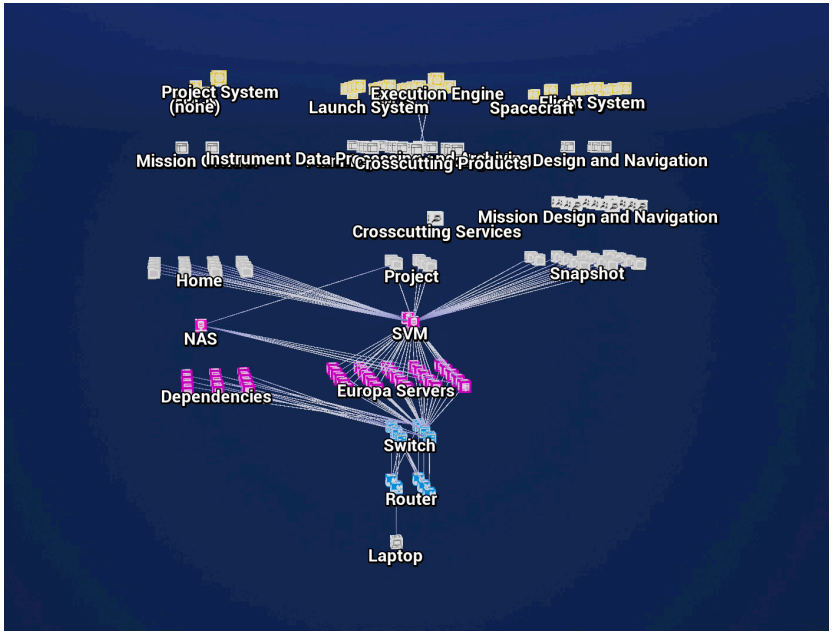
"Oil Derrick" by Nikita Kozin, from thenounproject.com
"Transmission Tower" by Arthur Shlain, from thenounproject.com
"Processor" by Creative Stall, from thenounproject.com

Past Challenges

- Risk assessments are usually table top exercises performed with outdated information, not enough information, and at too slow of a pace.
- Attempted to use MBSE tools such as MagicDraw and Tom Sawyer to little avail.
- Conducted an industry/academic product search to find an extensible software product to conduct cyber-risk assessments.
    - Lots of claims and published papers but could not find a COTS product

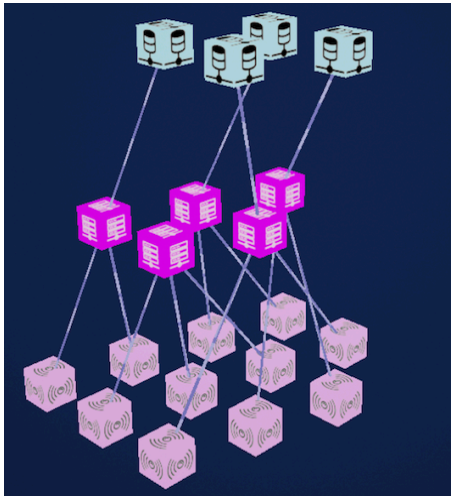
Cyber Analysis and Visualization Environment (CAVE)

- JPL-developed, extensible, software framework used by cyber defense analysts and project engineering staff
- Model and visualize the cyber-physical system of a project including:
  - Hardware, software, files, connections, mission objectives, and vulnerabilities
- Data sources used to generate a model include:
  - Host-based data, RedSeal, Nessus, Nexpose, Nmap, CVEs, L2-L3 mission objectives,
- Plug-in analysis architecture to run reasoning based analyses
  - For example, to determine if an adversary could traverse through the system to access a command file given known system vulnerabilities and then deploy a mitigation strategy.
- Generate reports of cyber-physical inventory for the mission
- Able to track likely adversary entry/paths/goals given known weaknesses in our project environments (i.e. CVEs, node centrality, proximity to the internet)
- Currently modeling missions in flight (Phase E) and development (Phase A, B, C/D)



Modeling and Analyses during Different Phases of the Project

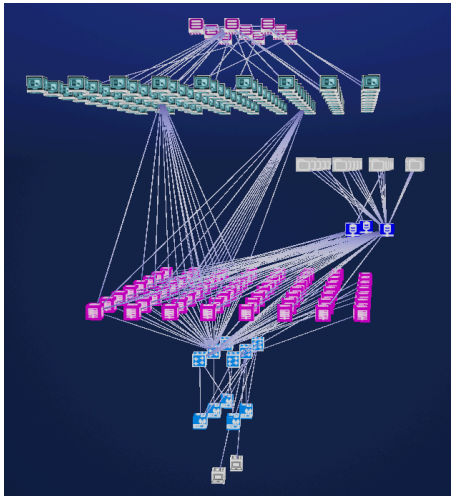
Phase A



Early Concept (Psyche)

- Security concepts and requirements

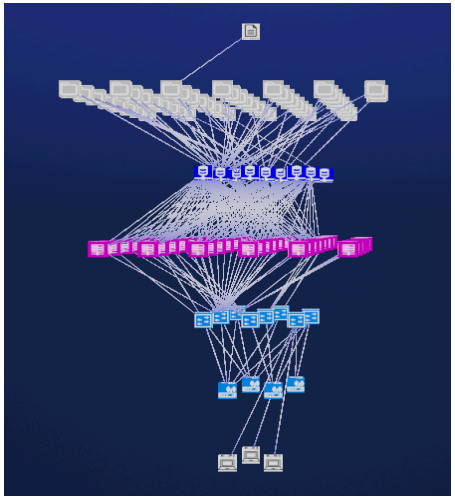
Phase C / D



Active Development (Europa)

- Inclusion of live systems Vulnerability and architectural analysis
- Detailed models analyzed by project personnel

Phase E



***Spacecraft Operations* (MSL)**

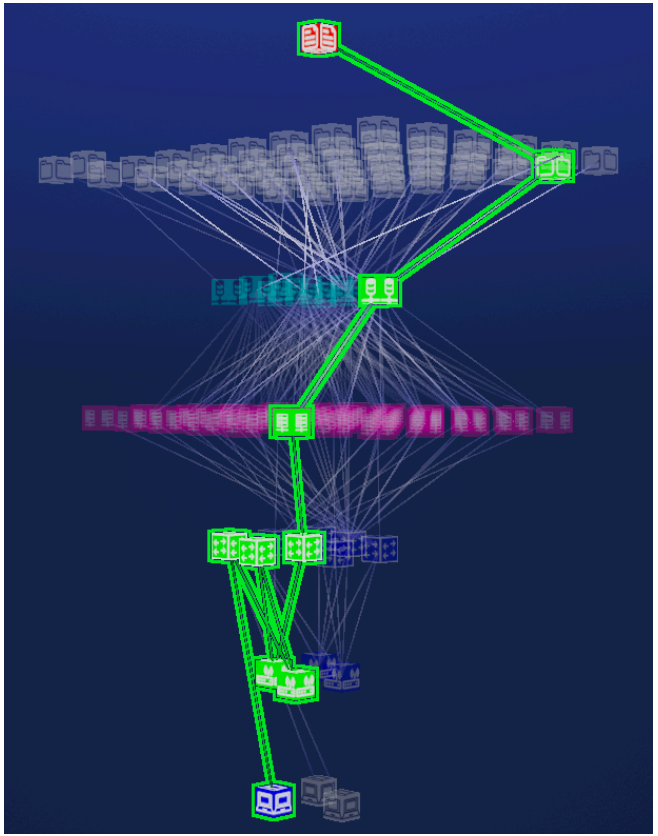
- Cybersecurity simulations of attack campaigns
- Mission architectures captured and catalogued in a library -- enabling lateral analyses of attack movement across several missions

Analyses in CAVE

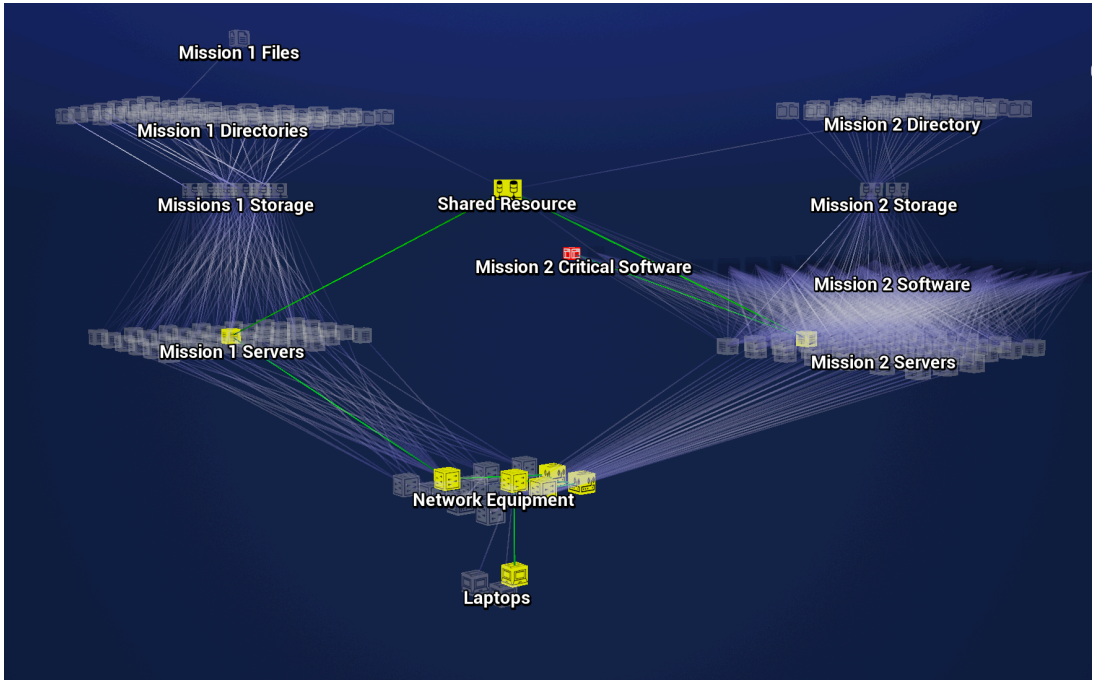
Short programs that allow CAVE users to interactively explore different aspects of their model.

Examples:

- On which ports can two servers communicate
- What mounted directories can a server read
- Any critical vulnerabilities on servers that can run a mission critical application
- What systems have a CVE



The Closest Threat Could Be Your Neighbor



Analysis of Horizontal Attack Paths between Projects Through an Obscured Shared Resource

Topics to Focus on

- How do we know we are capturing all the relevant data?
- What is the correct level of detail in building a model to perform an adequate risk assessment?
  - How do we account for known-unknowns and unknown-unknowns?
- How do we factor in mitigation strategies that can lower the risk?
  - Would like to evaluate different mitigations for their effectiveness and cost.
  - Finally, do a cost-benefit analysis to find an overall mitigation that maximizes the cost-benefit of all mitigation strategies.
- How do we quickly collect the information needed to conduct a cyber-risk assessment?
  - Do tools exist to collect and profile a system?

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov